The Set $\mathbb{K}[X]$

1 The Set $\mathbb{K}[X]$

1.1 Definition

Definition 1

A **polynomial** P with coefficients in K is any object of the form:

$$P = \sum_{k=0}^{n} a_k X^k$$

where $n \in \mathbb{N}$ and $a_0, \ldots, a_n \in \mathbb{K}$.
The numbers $a_0, \ldots, a_n$ are called the **coefficients** of P, and X is the **indeterminate**. The set of polynomials with coefficients in $\mathbb{K}$ is denoted by $\mathbb{K}[X]$.

Definition 2

Two polynomials $P = \sum_{k=0}^{n} a_k X^k$ and $Q = \sum_{k=0}^{n} b_k X^k$ in $\mathbb{K}[X]$ are **equal** if and only if they have the same coefficients:

$$P = Q \quad \iff \quad \forall k \in [0, n], \quad a_k = b_k$$

1.2 Algebraic Operations in $K[X]$

Definition 3

Let $P = \sum_{k=0}^{n} a_k X^k$ and $Q = \sum_{k=0}^{m} b_k X^k$ in $\mathbb{K}[X]$. Let $\lambda \in K$. We define:

- The **sum**:
$$P + Q = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k$$
where we assume $a_k = 0$ if $k > n$ and $b_k = 0$ if $k > m$.
- The **scalar multiplication**:
$$\lambda P = \sum_{k=0}^{n} (\lambda a_k) X^k$$
- The **product of polynomials**:
$$PQ = \sum_{k=0}^{n+m} c_k X^k, \quad \text{where } c_k = \sum_{l=0}^{k} a_l b_{k-l}$$

Proposition 1

Let $P, Q \in \mathbb{K}[X]$ and $\lambda \in \mathbb{K}$.

- $P + Q \in \mathbb{K}[X]$
- $\lambda P \in \mathbb{K}[X]$
- $PQ \in \mathbb{K}[X]$

Proposition 2

Let $P, Q, R \in \mathbb{K}[X]$ and let $\lambda \in \mathbb{K}$.

- $(PQ)R = P(QR)$ (Associativity of multiplication).
- $PQ = QP$ (Commutativity of multiplication).
- $P(Q + R) = PQ + PR$ (Distributivity of multiplication over addition).

Proposition 3: Binomial Theorem

Let $P, Q \in \mathbb{K}[X]$ and $n \in \mathbb{N}$, we have:

$$(P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k}.$$

Proposition 4: Factorization Formula

Let $P, Q \in K[X]$ and $n \in \mathbb{N}^*$, we have:

$$P^n - Q^n = (P-Q) \sum_{k=0}^{n-1} P^k Q^{n-1-k}.$$

Definition 4

Let $P = \sum_{k=0}^{n} a_k X^k \in K[X]$, $Q \in \mathbb{K}[X]$. The **composite polynomial**, denoted $P \circ Q$ or $P(Q)$, is defined by:

$$P \circ Q = \sum_{k=0}^{n} a_k Q^k.$$

Proposition 5

Let $P, Q, R \in \mathbb{K}[X]$ and $\lambda, \mu \in K$.

- $(\lambda P + \mu Q) \circ R = \lambda P \circ R + \mu Q \circ R$
- $(P \circ Q) \circ R = P \circ (Q \circ R)$
- $(P \circ Q) = R \circ (P \circ Q)$
- $X \circ P = P \circ X = P$

1.3 Degree of a Polynomial

Definition 5

Let $P = \sum_{k=0}^{m} a_k X^k \in \mathbb{K}[X]$. If P is not zero, the **degree of the polynomial** P is the greatest natural number n such that $a_n \neq 0$. We denote it:

$$\deg(P) = \max(k \in [0, n] \mid a_k \neq 0).$$

If $P = 0$, we set $\deg(P) = -\infty$ by convention. If $\deg(P) = n$, the coefficient a_n is called the **leading coefficient** of P. P is called **monic** if its leading coefficient is 1.

Definition 6

For $n \in \mathbb{N}$, we define $\mathbb{K}_n[X]$ as the set of polynomials of degree at most n:

$$\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg(P) \leq n\}.$$

1.4 Operations on Degrees

Proposition 6

Let $P, Q \in \mathbb{K}[X]$ and $\lambda \in \mathbb{K}$. Then:

1. $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$;
2. Furthermore, if $\deg(P) \neq \deg(Q)$, then $\deg(P + Q) = \max(\deg(P), \deg(Q))$;
3. If $\lambda \in K^*$, $\deg(\lambda P) = \deg(P)$, and if $\lambda = 0$, then $\deg(\lambda P) = -\infty$;
4. $\deg(PQ) = \deg(P) + \deg(Q)$;
5. If $n \in \mathbb{N}$, $\deg(P^n) = n \cdot \deg(P)$;
6. If $\deg(Q) \geq 1$, $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Corollary 1
Let $n \in \mathbb{N}$, $P, Q \in \mathbb{K}_n[X]$, and $\lambda, \mu \in K$. Then:

$$\lambda P + \mu Q \in K_n[X].$$

1.5 Polynomial Function

Definition 7

Let $n \in \mathbb{N}$ and $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. The function:

$$\mathbb{K} \to \mathbb{K}, \quad x \mapsto \sum_{k=0}^{n} a_k x^k,$$

is called the polynomial function associated with the polynomial P.

II Divisibility and Euclidean Division in $\mathbb{K}[X]$

2.1 Divisibility in $\mathbb{K}[X]$

Definition 8

Let $A, B \in \mathbb{K}[X]$. We say that B divides A in $\mathbb{K}[X]$, or that A is a multiple of B in $\mathbb{K}[X]$, and we denote $B \mid A$, if there exists $C \in \mathbb{K}[X]$ such that:

$$A = BC.$$

2.2 Euclidean Division in $K[X]$

Theorem 1: Euclidean Division
Let $A, B \in \mathbb{K}[X]$ such that $B \neq 0$. Then there exists a unique pair $(Q, R) \in (\mathbb{K}[X])^2$ such that:

$$A = BQ + R \quad \text{and} \quad \deg(R) < \deg(B).$$

Q is called the quotient and R the remainder in the Euclidean division of A by B.

Corollary 2
Let $A, B \in \mathbb{K}[X]$ with $B \neq 0$. We have: B divides A if and only if the remainder in the Euclidean division of A by B is zero.

III Derivation in $\mathbb{K}[X]$

3.1 Definition

Definition 9

Let $n \in \mathbb{N}$, and let $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. The derivative of P, denoted by P', is defined as:

$$P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{l=0}^{n-1} (l+1) a_{l+1} X^l.$$

Definition 10

Let $P \in \mathbb{K}[X]$. The successive derivatives of P are defined recursively as follows:

$$P^{(0)} = P \quad \text{and} \quad \forall n \in \mathbb{N},\, P^{(n+1)} = (P^{(n)})'.$$

Proposition 7

Let $n, k \in \mathbb{N}$. Then:

$$(X^n)^{(k)} = \begin{cases} \frac{n!}{(n-k)!} X^{n-k} & \text{if } k \leq n, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 8

Let $P \in \mathbb{K}[X]$, and let $k \in \mathbb{N}$. Then:

1. $\deg(P') = \begin{cases} \deg(P) - 1 & \text{if } \deg(P) \geq 1, \\ -\infty & \text{otherwise.} \end{cases}$

2. $\deg(P^{(k)}) = \begin{cases} \deg(P) - k & \text{if } \deg(P) \geq k, \\ -\infty & \text{otherwise.} \end{cases}$

Corollary 3

Let $P \in \mathbb{K}[X]$, and let $n \in \mathbb{N}$. Then:

$$\deg(P) \leq n \iff P^{(n+1)} = 0.$$

3.2 Operations on Derivatives

Proposition 9

Let $P, Q \in \mathbb{K}[X]$. Then:

1. Differentiation is linear: $\forall \lambda, \mu \in \mathbb{K}$, $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.
2. $(PQ)' = P'Q + PQ'$.

Proposition 10: Leibniz Formula

Let $P, Q \in \mathbb{K}[X]$, and let $n \in \mathbb{N}$. Then:

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Proposition 11

Let $P, Q \in \mathbb{K}[X]$. Then:

$$(P \circ Q)' = Q' \times (P' \circ Q).$$

3.3 Taylor's Formula

Proposition 12: Taylor's Formula

Let $P \in \mathbb{K}[X]$, and let $N \in \mathbb{N}$ such that $\deg(P) \leq N$. Let $a \in \mathbb{K}$. Then:

$$P(X) = \sum_{k=0}^{N} \frac{P^{(k)}(a)}{k!}(X - a)^k.$$

IV Roots

4.1 Definition

Definition 11

A scalar $a \in \mathbb{K}$ is said to be a **root** of a polynomial $P \in \mathbb{K}[X]$ if and only if $P(a) = 0$.

Proposition 13

Let $a \in \mathbb{K}$ and $P \in \mathbb{K}[X]$. Then:

- The remainder in the Euclidean division of P by $(X-a)$ is $P(a)$.
- a is a root of P if and only if $(X-a)$ divides P.

Corollary 4

Let $P \in \mathbb{K}[X]$, and let $a, b \in \mathbb{K}$ such that $a \neq b$. If a and b are roots of P, then $(X-a)(X-b) \mid P$.

Proposition 14

Let $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$, and let $a_1, a_2, \ldots, a_n \in \mathbb{K}$ be pairwise distinct. $a_1, a_2, \ldots, a_n$ are roots of P if and only if $\prod_{i=1}^{n}(X - a_i) \mid P$.

4.2 Number of Roots

Proposition 15

A nonzero polynomial of degree $n \in \mathbb{N}$ has at most n pairwise distinct roots.

Corollary 5

A polynomial in $\mathbb{K}[X]$ with at least $n+1$ pairwise distinct roots is the zero polynomial. The only polynomial with an infinite number of (distinct) roots is the zero polynomial.

4.3 Multiplicity

Definition 12

Let P be a nonzero polynomial in $\mathbb{K}[X]$, and let $a \in \mathbb{K}$ be a root of P. The **order of multiplicity** of the root a is defined as the largest integer $m \in \mathbb{N}^*$ such that $(X-a)^m$ divides P. In other words, $m \in \mathbb{N}^*$ such that:

$$(X-a)^m \mid P \quad \text{and} \quad (X-a)^{m+1} \nmid P.$$

We then say that a is a root of P of multiplicity m.

Proposition 16

Let $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, and $m \in \mathbb{N}^*$. a is a root of multiplicity m of P if and only if there exists $Q \in \mathbb{K}[X]$ such that $P = (X-a)^m Q$ and a is not a root of Q.

Corollary 6

Let $P \in \mathbb{K}[X]$, $P \neq 0$, and let $n = \deg(P)$. P has at most n roots, counted with their multiplicities.

Proposition 17

Let $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, and $m \in \mathbb{N}^*$. a is a root of multiplicity m of P if and only if, for all $k \in [\![0, m-1]\!]$, a is a root of $P^{(k)}$ and a is not a root of $P^{(m)}$.

Corollary 7

Let $P \in \mathbb{K}[X]$, and let $a \in \mathbb{K}$ be a root of multiplicity $m \in \mathbb{N}^*$ of P. Let $k \in [\![0, m-1]\!]$. Then a is a root of multiplicity $m-k$ of $P^{(k)}$.

4.4 Factorized Polynomials

Definition 13

Let $P \in \mathbb{K}[X]$ be a polynomial of degree $n \in \mathbb{N}^*$. P is said to be **factorized** if and only if there exist $\lambda \in \mathbb{K}^*$ and $a_1, \dots, a_n \in \mathbb{K}$ such that:

$$P = \lambda \prod_{j=1}^{n} (X - a_j).$$

Proposition 18

Let $P \in \mathbb{K}[X]$ be a polynomial of degree $n \in \mathbb{N}^*$. P is factorized in $\mathbb{K}$ if and only if there exist $\lambda \in \mathbb{K}^*$, $k \in \mathbb{N}^*$, and $a_1, \ldots, a_k \in \mathbb{K}$ pairwise distinct, such that:

$$P = \lambda \prod_{j=1}^{k} (X - a_j)^{m_j}.$$

Where:

- λ is the leading coefficient of P,
- The $a_j \in \mathbb{K}$ are the roots of P with multiplicities m_j,
- $\sum_{j=1}^{k} m_j = \deg(P)$.

V. Factorization into Irreducible Factors

5.1 Theorem of d'Alembert-Gauss

Theorem 2: d'Alembert-Gauss Theorem

Every non-constant polynomial in $\mathbb{C}[X]$ has at least one root in $\mathbb{C}$.

Corollary 8

- Every non-constant polynomial in $\mathbb{C}[X]$ is factorized.
- Every nonzero polynomial in $\mathbb{C}[X]$ of degree $n \geq 0$ has exactly n roots counted with their multiplicities.

5.2 Irreducible Polynomials

Definition 14

Let $P, Q \in \mathbb{K}[X] \setminus \{0\}$. P and Q are said to be **associated** if and only if there exists $\lambda \in \mathbb{K}^*$ such that $P = \lambda Q$.

Definition 15

A polynomial $P \in \mathbb{K}[X]$ is **irreducible** over $\mathbb{K}[X]$ if P is non-constant and its only divisors in $\mathbb{K}[X]$ are the nonzero constant polynomials (i.e., polynomials associated with 1) and polynomials associated with P.
Thus, a polynomial $P \in \mathbb{K}[X]$ is irreducible if and only if:

- P is non-constant.
- $\forall A \in \mathbb{K}[X],\ A \mid P \implies \exists \lambda \in \mathbb{K}^*, A = \lambda$ or $A = \lambda P$.

5.3 Irreducible Polynomials in $\mathbb{C}[X]$

Proposition 19

The irreducible polynomials in $\mathbb{C}[X]$ are the polynomials of degree 1.

Theorem 3

Let P be a nonzero polynomial in $\mathbb{C}[X]$. P can be uniquely written (up to the order of the factors) as a product of irreducible polynomials in $\mathbb{C}[X]$:

$$P = \lambda \prod_{k=1}^{n} (X - a_k)^{m_k},$$

where $n \in \mathbb{N}$, λ is the leading coefficient of P, $a_1, \ldots, a_n$ are the distinct roots of P, and $m_1, \ldots, m_n \in \mathbb{N}^*$ are their respective multiplicities.

5.4 Irreducible Polynomials in $\mathbb{R}[X]$

Proposition 20

The irreducible polynomials in $\mathbb{R}[X]$ are:

- Polynomials of degree 1.
- Polynomials of degree 2 whose discriminant is strictly negative.

Theorem 4

Let P be a nonzero polynomial in $\mathbb{R}[X]$. P can be uniquely written (up to the order of the factors) as a product of irreducible polynomials in $\mathbb{R}[X]$:

$$P = \lambda \prod_{i=1}^{p} (X - a_i)^{m_i} \prod_{j=1}^{q} \left(X^2 + b_j X + c_j\right)^{n_j},$$

where:

- $p, q \in \mathbb{N}$, $\lambda \in \mathbb{R}$ is the leading coefficient of P,
- $a_1, \ldots, a_p$ are the pairwise distinct real roots of P with respective multiplicities $m_1, \ldots, m_p \in \mathbb{N}^*$,
- $(b_1, c_1), \ldots, (b_q, c_q)$ are pairwise distinct real pairs such that for all $k \in \{1, \ldots, q\}$, $b_k^2 - 4c_k < 0$, and $n_1, \ldots, n_q \in \mathbb{N}^*$.

VI. Sum and Product of the Roots of a Polynomial

Proposition 21: Coefficient/Root Relations

Let $P \in \mathbb{K}[X]$ be a polynomial of degree $n \in \mathbb{N}^*$, factored over $\mathbb{K}[X]$ with roots $x_1, \ldots, x_n$ (each root being repeated according to its multiplicity).
If $P = \sum_{k=0}^{n} a_k X^k$ (where $a_n \neq 0$), then:

$$\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n} \quad \text{and} \quad \prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}.$$